CLAIMS

What is claimed is:

1. An apparatus, comprising:

a detector to determine whether a first radio frequency identification tag read by a reader that reads radio frequency identification tags is a match with a second radio frequency identification tag read by said reader.

2. An apparatus as claimed in claim 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag.

3. An apparatus as claimed in claim 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector authenticates the lock tag when said detector detects the lock tag and the key tag being within a predetermined distance of said detector.

4. An apparatus as claimed in 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector includes a nonce generator to generate a nonce, an encryptor to encrypt a nonce using a public cryptography key received from the lock tag to provide an encrypted nonce to the key tag, and a comparator to compare a nonce generated by the nonce generator with a decrypted version of the encrypted nonce that was decrypted using a private cryptography key of the key tag.

5. An apparatus as claimed in claim 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector includes a nonce generator to generate a nonce, and a comparator to compare an encrypted version of the nonce encrypted using a cryptography key of the lock tag with an encrypted version of the nonce encrypted using a cryptography key of the key tag.

6. An apparatus as claimed in claim 5, wherein the cryptography key of the lock tag is the same as the cryptography key of the key tag.

7. An apparatus as claimed in claim 5, wherein the nonce generator generates a series of nonces, wherein the lock tag delays encryption of the nonce with respect to encryption of the nonce by the key tag, and wherein said detector further comprises a delay to delay the encrypted version of the nonce encrypted by the key tag.

8. An apparatus as claimed in claim 1, wherein said detector determines whether the first radio frequency identification tag is a match with the second radio frequency identification tag or a third or more radio frequency identification tags.

9. A method, comprising:

programming a first radio frequency identification tag; and

programming a second radio frequency identification tag to be associated with the first radio frequency identification tag.

10. A method as claimed in claim 9, wherein the first radio frequency identification tag is programmed to have a public encryption key and wherein the second radio frequency identification tag is programmed to have a private encryption key.

11. A method as claimed in claim 9, wherein the first radio frequency identification tag is programmed to have the same cryptography key as the second radio frequency identification tag.

12. A method as claimed in claim 9, wherein said programming a first radio frequency identification tag occurs at a different time than said programming a second radio frequency identification tag.

13. A method as claimed in claim 9, further comprising programming a third or more radio frequency identification tags to be associated with the first radio frequency identification tag.

14. A method, comprising:

generating a nonce;

encrypting the nonce using a cryptography key received from a first radio frequency identification tag to result in an encrypted nonce;

sending the encrypted nonce to a second radio frequency identification tag that decrypts the encrypted nonce to result in a decrypted nonce;

receiving the nonce from the second radio frequency identification tag; and

comparing the nonce generated by said generating to the decrypted nonce.

15. A method as claimed in claim 14, further comprising determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

16. A method as claimed in claim 14, wherein the cryptography key received from the first radio frequency identification tag is a public key, and wherein the second radio frequency identification tag decrypts the encrypted nonce using a private key associated with the public key.

17. A method, comprising:

generating a series of nonces;

sending the series of nonces to a first radio frequency identification tag and a second radio frequency identification tag;

receiving encrypted versions of the series of nonces from the first and second radio frequency identification tags; and

comparing the encrypted versions of the series of nonces received from the first radio frequency identification tag with the encrypted versions of the series of nonces received from the second radio frequency identification tag.

18. A method as claimed in claim 17, further comprising determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

19. A method as claimed in claim 17, wherein the first and second radio frequency identification tags encrypt the series of nonces using the same cryptography key.

20. A method as claimed in claim 17, wherein the first radio frequency radio identification tag delays the series of nonces with respect to the second radio frequency identification tag, and further comprising delaying the encrypted versions of the series of nonces received from the second radio frequency identification tag prior to said comparing.

21. An article comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in association of at least two or more radio frequency identification tags by:

programming a first radio frequency identification tag; and

programming a second radio frequency identification tag to be associated with the first radio frequency identification tag.

22. An article as claimed in claim 21, wherein the first radio frequency identification tag is programmed to have a public encryption key and wherein the second radio frequency identification tag is programmed to have a private encryption key.

23. An article as claimed in claim 21, wherein the first radio frequency identification tag is programmed to have the same cryptography key as the second radio frequency identification tag.

24. An article as claimed in claim 21, wherein said programming a first radio frequency identification tag occurs at a different time than said programming a second radio frequency identification tag.

25. An article as claimed in claim 21, wherein the instructions, when executed, further result in association of at least two or more radio frequency identification tags by programming a third or more radio frequency identification tags to be associated with the first radio frequency identification tag.

26. An article comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in verification of association of at least two or more radio frequency identification tags by:

generating a nonce;

encrypting the nonce using a cryptography key received from a first radio frequency identification tag to result in an encrypted nonce;

sending the encrypted nonce to a second radio frequency identification tag that decrypts the encrypted nonce to result in a decrypted nonce;

receiving the nonce from the second radio frequency identification tag; and

comparing the nonce generated by said generating to the decrypted nonce.

27. An article as claimed in claim 26, wherein the instructions, when executed, further result in verification of association of at least two or more radio frequency identification tags by determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

28. An article as claimed in claim 26, wherein the cryptography key received from the first radio frequency identification tag is a public key, and wherein the second radio frequency identification tag decrypts the encrypted nonce using a private key associated with the public key.

29. An article comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in verification of association of at least two or more radio frequency identification tags by:

generating a series of nonces;

sending the series of nonces to a first radio frequency identification tag and a second radio frequency identification tag;

receiving encrypted versions of the series of nonces from the first and second radio frequency identification tags; and

comparing the encrypted versions of the series of nonces received from the first radio frequency identification tag with the encrypted versions of the series of nonces received from the second radio frequency identification tag.

30. An article as claimed in claim 29, wherein the instructions, when executed, further result in verification of association of at least two or more radio frequency identification tags by determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

31. An article as claimed in claim 29, wherein the first and second radio frequency identification tags encrypt the series of nonces using the same cryptography key.

32. An article as claimed in claim 29, wherein the first radio frequency radio identification tag delays the series of nonces with respect to the second radio frequency identification tag, and wherein the instructions, when executed, further result in verification of association of at least two or more radio frequency identification tags by comprising delaying the encrypted versions of the series of nonces received from the second radio frequency identification tag prior to said comparing.

33. An apparatus, comprising:

a transceiver to communicate with a radio frequency identification tag;

a directional antenna coupled to said transceiver; and

a detector to determine whether a first radio frequency identification tag read by said transceiver is a match with a second radio frequency identification tag read by said transceiver.

34. An apparatus as claimed in claim 33, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag.

35. An apparatus as claimed in claim 33, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector authenticates the lock tag when said detector detects the lock tag and the key tag being within a predetermined distance of said detector.

36. An apparatus as claimed in claim 33, wherein said detector determines whether the first radio frequency identification tag is a match with the second radio frequency identification tag or a third or more radio frequency identification tags.